IN THE CLAIMS

Please amend the claims as follows:

1. – 5. (Canceled.)

6. (Currently Amended) A private, secure wide area network using the internet as a backbone between a source site and a destination site, comprising:

a first dedicated signal path to a router of a source ISX/ISP provider of internet access;

a source router located at a source site and having a channel service unit having an output coupled to said first dedicated signal path and having a routing table which has been configured to recognize AlterWAN packets and always route them over said first dedicated signal path to said source ISX/ISP provider, said AlterWAN packets being packets having as their destination address one of one or more predetermined Internet Protocol addresses assigned to an AlterWAN private tunnel, and AlterWAN private tunnel being a data path through the internet which uses only high bandwidth, low latency data paths between predetermined ISX/ISP provider sites which have been pre-tested to ensure that adequate bandwidth and low latency exists for AlterWAN packets and that AlterWAN packets are always routed at said predetermined ISX/ISP provider site into said AlterWAN private tunnel;

a source firewall circuit located at a source site and having a first port for coupling directly or through a local area network to one or more computers or other devices at said source site for which communication over said private, secure wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encapsulate any Internet Protocol packets hereafter IP packets transmitted from said first computer or other device which have a destination Internet Protocol address (hereafter IP address) which is one of a set of "predetermined IP addresses", said predetermined IP addresses" being IP addresses of computers or other devices at a destination site which are assigned to said private tunnel, said encapsulation being performed on the payload sections of IP packets having as their destination address one of said "predetermined IP addresses", hereafter referred to as AlterWAN packets and for encrypting

said payload sections of said AlterWAN packets using any encryption method known to a destination firewall at a destination site and transmitting said AlterWAN packets to said source router, but said source firewall for not encapsulating any IP packets transmitted by said first computer or other device which do not have as their destination address one of said "predetermined IP addresses", and for receiving incoming IP packets from various sources including computers and devices at said destination site via said source router and for recognizing AlterWAN packets among these IP packets on the basis that an AlterWAN packet has one of said "predetermined IP addresses" as its destination address, and decrypting the payloads of said AlterWAN packets to recover said IP packets that were encapsulated in said AlterWAN packets and transmitting at least said recovered IP packets to said one or more computers or devices at said source site to which said recovered IP packets are addressed;

one or more internet data paths coupled to routers of said predetermined ISX/ISP providers of internet services, said routers having their routing tables configured to recognize said AlterWAN packets by their destination addresses and to cause said routers to route AlterWAN packets into said AlterWAN private tunnel data path, each said predetermined ISX/ISP provider being a provider of internet services who has contracted to provide routing of AlterWAN packets into said AlterWAN private tunnel data path, said AlterWAN private tunnel data path being at least one of said internet data paths which has been pre-tested to verify that said data path does in fact ~~provides~~ provide a low hop count data path having an average available bandwidth along each portion of said data path travelled by said AlterWAN packets which exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source site and said destination site;

a destination router including a channel service unit coupled to or part of said destination router and having a trusted side output, said destination router coupled through said channel service unit and a second dedicated data path to a router of a said participating ISX/ISP provider, said destination router having its routing tables configured to recognize said AlterWAN packets and route them to said trusted side output;

a destination firewall circuit having a WAN interface coupled to said trusted side output of said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to [[a]] one or more computers or devices for

which communication across said private AlterWAN data path is desired, said destination firewall functioning to encapsulate into the payload sections of AlterWAN packets IP packets transmitted from said one or more computers or devices at said destination site and having as their destination addresses one of said "predetermined IP addresses" which is an IP address of said one or more computers or devices at said source site, and functioning to encrypt the payloads of said AlterWAN packets and transmit said AlterWAN packets to said destination router, but for not encapsulating into AlterWAN packets any IP packets transmitted from said one or more computers or devices at said destination site which do not have as their destination address one of said "predetermined IP addresses" and for receiving IP packets from various sources including said one or more computers or devices at said source site via said destination router, and functioning to recognize AlterWAN packets among said received IP packets and decrypt the payload sections of said AlterWAN packets to recover the original IP packets and transmitting at least the decrypted IP packets recovered from AlterWAN packet to said one or more computers or devices at said destination site.

7. (Currently Amended) A process for sending AlterWAN data packets securely between a computer at a source site and a computer at a destination site so as to implement a private Wide Area Network (hereafter AlterWAN) between said source and destination sites of a customer, said AlterWAN using the internet as a backbone but which is private and which only said customer can use comprising the steps:

receiving at a source firewall incoming Internet Protocol packets (hereafter IP packets) from a computer at a source site of a customer, some of said IP packets having as their destination addresses an Internet Protocol address (hereafter IP address) which is one of one or more IP addresses of one or more computers or other computing devices at a destination site of said customer;

at said source firewall, comparing the destination address in each said received IP packet to an IP address of a computer at said destination site of said customer, and if an IP packet has as its destination address the IP address of a computer or other computing device at said destination site (hereafter referred to as an AlterWAN inner packet), concluding said IP packet is an AlterWAN inner packet which needs to be transmitted to said computer or other computing

device at said destination site via a high bandwidth, low latency, low hop count data path using said internet as a backbone and connecting said source site to said destination site and having an average available bandwidth which exceeds the worst case bandwidth consumption of packets traveling between said source site and said destination site (hereafter referred as the AlterWAN data path), but if said destination address of said received IP packet is not an IP address of a computer or other computing device at said destination site, concluding said IP packet is an AlterWAN inner packet and needs to be routed like any other IP packet would be routed;

if said received IP packet is an AlterWAN inner packet, encapsulating said AlterWAN inner packet into the payload section of a second IP packet having as its destination address the IP address of an untrusted side of a firewall at said destination site of said AlterWAN data path (hereafter referred to as composite AlterWAN packet) and encrypting at said source firewall at least a payload portion of said AlterWAN inner packet using any encryption algorithm which can be decrypted by said firewall at said destination site, and forwarding said composite AlterWAN packet to a source router;

if said received IP packet is not an AlterWAN inner packet, forwarding said received IP packet (hereafter referred to as a non-AlterWAN packet) to said source router without encapsulating said non-AlterWAN packet into a composite AlterWAN packet;

at said source router, converting both said composite AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated signal path coupling said source router to a predetermined source participating ISX/ISP provider of internet connectivity and routing services, and transmitting said signals to said predetermined source participating ISX/ISP provider, said predetermined source participating ISX/ISP provider being selected because said provider has available a high bandwidth, low latency, low hop count data path which is part of said AlterWAN data path and also has agreed to route said ~~chomposite~~ composite AlterWAN packets into said AlterWAN data path and has routers which either already contain routing statements ~~wich~~ which will route said AlterWAN packets into said AlterWAN data path or which have been configured to contain such a routing statement or statements.

8. (Previously Presented) An apparatus comprising:

a dedicated data path for coupling signals to a specially selected first participating ISX/ISP provider of internet access;

a first firewall circuit having a first port for coupling directly or through a local area network to one or more computing devices for which is desired communication over a private wide area network between a customer's source site and destination site using the internet as a backbone, and having a second port, said firewall functioning to use the destination addresses in the headers of each packet received from said one or more computing devices at said source site to distinguish between conventional packets and AlterWAN payload packets, where AlterWAN payload packets are packets having as their destination addresses an address of a computing device at said destination site or said source site, and wherein a computing device at said destination site is coupled to a computer at said source site via a second firewall circuit and an AlterWAN data path comprising of a virtual private network tunnel implemented along a high bandwidth, low latency, low hop count data paths through a public wide area network such as the internet terminating at said source site at an untrusted side of said first firewall circuit and terminating at said destination site at an untrusted side of said second firewall circuit, and wherein conventional packets are packets which are not addressed to any computing device at said destination site, said first firewall circuit functioning to encapsulate said AlterWAN payload packets in the payload section of AlterWAN packets which have as their destination address the address of said untrusted side of said second firewall circuit at said destination end of said virtual private network tunnel, said first firewall circuit further functioning to encrypt the payloads (AlterWAN payload packet) of AlterWAN packets and distinguishing between incoming AlterWAN packets from said destination site and conventional packets by comparing the destination addresses thereof to the address of said untrusted side of said first firewall circuit and concluding that any incoming packets addressed to said first firewall circuit are AlterWAN packet and all packets addressed to one or more computing devices at said source site coupled to said first firewall circuit are conventional packets, and further functioning to decrypt the payload sections of any incoming AlterWAN packets so as to recover the encapsulated AlterWAN payload packet;

a source router having an input coupled to said second port of said first firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said router and channel service unit functioning to receive said AlterWAN packets and said conventional packets from said first firewall circuit and convert said packets into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWAN packets and conventional packets received from said first firewall over said dedicated data path to said specially selected first participating ISX/ISP provider where said AlterWAN packets will be routed via said AlterWAN data path to said second firewall and wherein said AlterWAN data path has an average available bandwidth which substantially exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site.

9. (Currently Amended) A method of designing and implementing a private wide area network using the internet as a backbone carrying data packets between a source site to a destination site hereafter referred to as an AlterWAN data path), comprising the steps:

1) selecting source and destination sites that have computers or other devices (hereafter referred to simply as computers) that need to be connected by a wide area network;

2) examining available ISX/ISP internet service providers that can route packets between said source and destination sites and selecting two or more of such ISX/ISP providers as participating ISX/ISP providers including at least a source ISX/ISP provider and a destination ISX/ISP provider through which packet data passing between said source and destination sites will be routed, said selection of said participating ISX/ISP providers being made upon the availability to said participating ISX/ISP providers of one or more high bandwidth, low latency data paths which will form part of said AlterWAN data paths, said participating ISX/ISP providers agreeing to route packets ~~travelling~~ traveling between said source site and said destination site (hereafter AlterWAN packets) into said AlterWAN data path and agreeing to allow route statements to be added to their routers to cause AlterWAN packets to always be routed into said AlterWAN data path, said participating ISX/ISP providers also agreeing to manage their portions of said AlterWAN data path so as to guarantee that the average available

bandwidth of their portion of said AlterWAN data path is substantially greater than the worst case bandwidth consumption of AlterWAN packet traffic between said source and destination sites;

3) adding route statements to routers of said participating ISX/ISP providers which will to cause AlterWAN packets to always be routed into said AlterWAN data path and pretesting said ISX/ISP providers selected in step 2 by testing to verify the data path that AlterWAN packets travel will be a portion of said AlterWAN data path and that performance is adequate;

4) contracting to establish and establishing a first dedicated signal path between the output of a source router at which said signals appear and said source ISX/ISP provider in said group of participating ISX/ISP providers selected in step 2, said first dedicated signal path having sufficiently high bandwidth to handle the worst case traffic volume in AlterWAN packets;

5) contracting to provide a second dedicated signal path connecting the input of a destination router to said destination ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume in AlterWAN packets;

6) coupling an untrusted port of a source firewall/virtual private network circuit (hereafter referred to as the source firewall) to a source router and coupling a trusted port of said source firewall to one or more computing device or devices at said source site and configuring said source firewall to examine the destination addresses of a first internet Protocol packet (hereafter IP packet) received from one of one or more computing devices at said source site and encapsulating each first IP packet having as its destination address and address which is a Internet Protocol address (hereafter IP address) of any computing device at said destination site as a payload portion in a second IP packet, said second IP packet hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of a destination firewall/virtual private network circuit (hereafter referred to as the destination firewall) at said destination site and having an encrypted version of at least the payload section of said first IP packet as its payload, said source firewall being configured to recognize non AlterWAN packets and with portions of said AlterWAN packet other than said

payload section being referred to herein as an AlterWAN packet header not to encapsulate or encrypt the payload portions of any non AlterWAN packets received from one or ~~mor~~ more of said devices at said source site which do not have as their destination address an IP address of any device at said destination site, and configuring said source firewall to screen incoming IP packets from said destination firewall so as to recognize any incoming AlterWAN packets which have as their destination addresses the IP address of the untrusted port of said source firewall and to strip off said AlterWAN packet headers and decrypt a payload portion of each said incoming AlterWAN packet to recover the original IP packet transmitted from said destination firewall so as to recover the original IP packet transmitted to said destination firewall by a computer at said destination site, and for outputting said recovered original IP packet to said device or devices at said source site having the IP address which is the destination address of said original IP packet;

7) coupling a source router to receive said AlterWAN packets and non-AlterWAN packets from said source firewall and to convert said AlterWAN and non-AlterWAN packets in a channel service unit to signals suitable for transmission over said first dedicated signal path to said source ISX/ISP provider;

8) providing a destination router at said destination site having a firewall port coupled to an untrusted port of said destination firewall and having a channel service unit coupled to said destination ISX/ISP provider via said second dedicated signal path and configuring said destination router to receive from said second dedicated signal path downstream signals encoding both encrypted AlterWAN packets and conventional non AlterWAN IP packets and convert said signals back into the original digital IP packet form, and configuring said destination router to output said recovered downstream IP packets at said firewall port coupled to said untrusted port of said destination firewall, and configuring said destination router to receive upstream AlterWAN packets and conventional non AlterWAN packets and convert both types of said packets into signals suitable for transmission on said second dedicated signal path coupling said destination router to said participating destination ISX/ISP provider in said group of participating ISX/ISP providers selected in step 2, and configuring said router to transmit said signals on said second dedicated signal path;

9) providing said destination firewall having an untrusted port coupled to said firewall port of said destination router so as to receive said recovered digital IP packets, and

configuring said destination firewall to recognize as AlterWAN packets incoming recovered IP packets having as their destination address the IP address of said destination firewall untrusted port and further configuring said destination firewall to strip off said AlterWAN packet header of each said AlterWAN packet and, as to each AlterWAN packet, decrypting a payload portion of said AlterWAN packet so as to recover said first IP packet which encapsulated in said AlterWAN packet, and configuring said destination firewall to output said first IP packet recovered from said AlterWAN packet by said decryption process and output each said first IP packet so recovered at an output coupled to one or more computing devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream first IP packets received from said one or more computing devices at said destination site and encapsulate each upstream first IP packet addressed to any computer or other computing device at said source site as a payload portion of a second IP packet, hereafter referred to as an upstream AlterWAN packet (an AlterWAN packet traveling from said destination site toward said source site), each said upstream AlterWAN packet having as its destination address the IP address of said untrusted port of said source firewall at said source site and a first IP packet as its payload, and further configuring said ~~said~~ destination firewall to encrypt the payload portions of each said upstream AlterWAN packet but not to encapsulate or encrypt payload portions of any non AlterWAN IP packets received from said one or more computing devices at said destination site, said non AlterWAN IP packets being those IP packets which do not have as their destination addresses an IP address of any device at said source site, and configuring said destination firewall to transmit said encrypted upstream AlterWAN packets and said conventional non AlterWAN packets to said destination router via said untrusted port.

10. (Currently Amended) A private wide area network connecting a customer source site to a customer destination site and using the internet as a backbone, comprising:

a first dedicated data path coupled to a first participating ISX/ISP provider of internet access;

a source router having a channel service unit having an output coupled to said first dedicated data path and configured with route statements that recognize IP packets addressed to the untrusted side of a destination firewall at said customer destination site (hereafter outgoing

AlterWAN packets) and cause said outgoing AlterWAN packets to be routed into an AlterWAN data path, wherein said AlterWAN data path is a high bandwidth, low latency data path from said customer source site to said customer destination site and back having an average available bandwidth that exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source and destination sites;

a source firewall having a first port for coupling directly or through a local area network to one or more devices at a customer source site, and having an untrusted port coupled to said source router directly or through a local area network, said untrusted port of said source firewall having an Internet Protocol address (hereafter IP address), said source firewall functioning to receive Internet Protocol packets (hereafter IP packets) from said one or more devices at said customer source site which are addressed to one or more devices at a customer destination site (hereafter AlterWAN payload packets) and other IP packets addressed to other locations on the internet (hereafter conventional IP packets), and for encapsulating said AlterWAN payload packets as the payload sections of ~~outgoign~~ outgoing AlterWAN packets which have as their destination addresses the IP address of an untrusted port of a destination firewall at said customer destination site (hereafter outgoing AlterWAN packets) and functioning to encrypt the payloads of said outgoing AlterWAN packets, and for receiving incoming IP packets and comparing the destination addresses of said incoming IP packets to said IP address of said untrusted port of said source firewall circuit any said incoming IP packet having as its destination address the IP address of said untrusted port of said source firewall being [[a]]an incoming AlterWAN packet, each said ~~incoming~~ incoming AlterWAN packet encapsulating as its payload section a AlterWAN payload packet, and decrypting the payload sections of any incoming AlterWAN packets so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload packet to a device at said customer source site to which said AlterWAN payload packet is addressed;

one or more routers of participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers of said ISX/ISP providers functioning to implement said AlterWAN data path as a high bandwidth, low latency, low hop count data path having an average available bandwidth that exceeds the worst case bandwidth consumed by incoming and outgoing AlterWAN packets ~~travelling~~ traveling between said source

and destination sites and configured to recognize said incoming and outgoing AlterWAN packets by their destination addresses and route them into said AlterWAN data path,

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated datapath to said router of said endpoint participating ISX/ISP provider and configured to recognize said outgoing AlterWAN packets arriving from said endpoint participating ISX/ISP provider which have ~~travelled~~ traveled from said source firewall via said AlterWAN data path and route them to said destination firewall, and configured to recognize said incoming AlterWAN packets from said destination firewall circuit and route them to said endpoint participating ISX/ISP provider;

said destination firewall circuit having an untrusted port having an IP address to which said outgoing AlterWAN packets are addressed, said untrusted port coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to one or more devices at said customer destination site, said destination firewall circuit configured so as to receive IP packets from said one or more devices at said customer destination site which are addressed to one or more devices at said customer source site (hereafter AlterWAN payload packets) and functioning to receive other conventional IP packets not addressed to any of the said devices at said customer source site, and for encapsulating said AlterWAN payload packets as the payload sections of AlterWAN packets addressed to said IP address of an untrusted port of said source firewall circuit at said customer source site (hereafter incoming AlterWAN packets) and functioning to encrypt the payloads of said incoming AlterWAN packets and for receiving incoming AlterWAN packets and comparing the destination addresses of said incoming AlterWAN packets to said IP address of said untrusted port of said destination firewall circuit, and decrypting the payload sections of any incoming AlterWAN packets having as their destination address the IP address of said untrusted port of said destination firewall circuit so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload packet to the device to which it is addressed at said customer destination site.

11. (Previously Presented) A method of doing business to establish a private bidirectional wide area network between a source site and a destination site using the internet as a backbone, comprising the steps:

connecting one or more computing devices at a source site to a firewall and source router and obtaining a known IP address for each computing device at said source site;

connecting one or more computing devices at a destination site to a firewall and destination router and obtaining a known IP address for each computing device at said destination site;

selecting one or more participating ISX/ISP internet service providers which have one or more high bandwidth, low latency, low hop count data paths that can be used as at least part of a high bandwidth, low latency, low hop count data path for transmission of AlterWAN data packets between said source site and said destination site (hereafter referred to as the AlterWAN data path), and making agreements with said participating ISX/ISP internet service providers to always route AlterWAN packets into said AlterWAN data path such that said AlterWAN data packets will only travel on AlterWAN data path, wherein said AlterWAN packets are defined as packets which contain as a destination address one of said known IP addresses of computing devices at said source site or said destination site, and ensuring that said routing tables of routers of said one or more participating ISX/ISP internet service providers either already contain routing statements that will cause AlterWAN packets to be routed into said AlterWAN data path or are modified to contain such route statements;

connecting said source router and said destination router to one of said participating ISX/ISP internet service providers through dedicated high bandwidth, low latency data paths.

12. (Previously Presented) A method comprising:

generating an Internet Protocol data packet (hereafter IP packet) having as its destination address an Internet Protocol address assigned to a computing device at the other end of a private, wide area network using the internet as a backbone (hereafter referred to as an AlterWAN private tunnel);

encrypting a payload portion of said IP packet to generate an encrypted IP packet;

generating a composite AlterWAN packet by encapsulating said encrypted IP packet in another IP packet having as its destination address an IP address of an untrusted side of a firewall which is at a destination site which is part of said AlterWAN private tunnel; and

routing said composite AlterWAN packet using a source router whose routing table has been configured to include a routing statement which recognizes said destination address of said composite AlterWAN packet and routes said composite AlterWAN packet via a dedicated data path to an AlterWAN data path, said AlterWAN data path being defined as a high bandwidth, low latency, low hop count data path provided by one or more participating ISX/ISP internet service providers that links said source site and said destination site of said AlterWAN private tunnel, each participating ISX/ISP internet service provider being one which has been selected as having at least one high bandwidth, low latency, low hop count data path which can be used to transmit said composite AlterWAN data packet either from said source site to said destination site or to another participating ISX/ISP internet service provider and which has routers which either already contain or which are configured to contain predetermined routing statements when said participating ISX/ISP agrees to provide routing services as part of said AlterWAN data path, said predetermined routing statements being ones which will recognize said IP destination address of each said composite AlterWAN data packets and cause said composite AlterWAN packets to be routed into said AlterWAN data path.

13. (Canceled).

14. (Previously Presented) A method of doing business comprising:

selecting one or more participating ISX/ISP internet service providers which have one or more high bandwidth, low latency, low hop count data paths that can be used as at least part of a high bandwidth, low latency, low hop count data path for transmission of composite AlterWAN data packets between a source site and a destination site of a private wide area network using the internet as a backbone (hereafter referred to as the AlterWAN data path), where composite AlterWAN data packets are defined as internet protocol packets (hereafter the outer packet) which encapsulate other internet protocol packets (hereafter the inner packet), said inner packet having as its destination address the IP address of a computing device at one end of said

AlterWAN data path and at least the payload section of said inner packet being encrypted, said outer packet having as its destination address an IP address of an untrusted side of a firewall at the same end of said AlterWAN data path as said computing device which has as its IP address said destination address of said inner packet;

making agreements with said participating ISX/ISP internet service providers to always route composite AlterWAN packets into said AlterWAN data path such that said composite AlterWAN data packets will only travel on said AlterWAN data path;

ensuring that said routing tables of routers of said one or more participating ISX/ISP internet service providers either already contain routing statements that will cause said composite AlterWAN data packets to be recognized and routed into said AlterWAN data path or are modified to contain such route statements.

15. (Previously Presented) A method of doing business comprising:

selecting one or more participating ISX/ISP internet service providers which have one or more high bandwidth, low latency, low hop count data paths that can be used as at least part of a high bandwidth, low latency, low hop count data path for transmission of AlterWAN data packets between a source site and a destination site of a wide area network using the internet as a backbone (hereafter referred to as the AlterWAN data path), where AlterWAN data packets are defined as internet protocol packets which contain as a destination address one of said known IP addresses of computing devices at said source site or said destination site;

making agreements with said participating ISX/ISP internet service providers to always route said AlterWAN packets into said AlterWAN data path such that said AlterWAN data packets will only travel on said AlterWAN data path;

ensuring that said routing tables of routers of said one or more participating ISX/ISP internet service providers either already contain routing statements that will cause said AlterWAN data packets to be recognized and routed into said AlterWAN data path or are modified to contain such route statements.

16 - 19. (Canceled).